OPERATIONS WORKPROGRAM CHAPTER 13WP

(FILE NAME ON DISK #3 = IS–WP#08.WPD) ***COMMENTS***

This section is intended to review the physical and functional aspects of the data centers operations for the presence of adequate procedures and controls. The work program should be used with the Operations Section narrative, which provides overall guidance. Also obtain access to reference manuals as an aid in performing the examination. Manuals with titles such as "Planning and Installation Guide," "Operational Principles," "Administrative Guide," and "Auditors Guide" can be particularly helpful. This section is used to review compliance with established policy and assess the soundness of physical and internal controls. The examination procedures in this workprogram should be coordinated with those in the Corporate Contingency Planning (Chapter 10) and the Security Physical and Data (Chapter 14) workprograms. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*. This document will become part of the workpapers.

Tier I

GENERAL

1. Identify the hardware and the operating system(s) in use.

MANAGEMENT REPORTING AND PLANNING

2. Review and evaluate the method(s) and frequency for monitoring system performance. This could entail:

   a. Monitoring continuously (if this is a large facility),

   b. Measuring whenever there is a change in the system configuration, or

   c. Measuring periodically to account for changes in loading (due for instance to increasing account volume).

3. In connection with systems performance monitoring and capacity planning, determine whether hardware/software constraints (choke points) have been identified, and evaluate their effect on operations.

4. Determine whether a job-accounting system is utilized.

PHYSICAL ENVIRONMENT

5. Does the computer room have an adequate and safe fire-suppression system with associated detectors

(heat, smoke, water), and are other necessary environmental controls in use?

6. Identify any obvious safety hazards to people or equipment.

7. Review the adequacy of the UPS system.

8. Determine if sensitive forms, negotiable items (checks, stock certificates, etc.), and signature plates are adequately controlled.

EQUIPMENT MAINTENANCE

9. Review log for equipment malfunctions.

10. Determine the existence of a program of regular preventive maintenance.

11. If any equipment is maintained by an outside vendor, review the maintenance agreement for reasonableness.

12. Review the performance of the maintenance vendors. If not, satisfactory, identify the corrective action.

OPERATIONAL PROCEDURES

13. Review the experience levels and training provided to the computer operations staff.

14. Review the operations procedures manual used by computer operators. Determine whether, according to those procedures and in practice, operator duties are properly segregated.

15. Review the console log. Determine whether it is reviewed by supervisory personnel and retained for a reasonable of time in safe storage to provide an audit trail.

16. Review the job scheduling function and assess its adequacy.

17. Review the problem reporting/resolution tracking system and determine whether:

    a. Problems are appropriately logged and prioritized

    b. Corrective measures are implemented in a timely manner.

c. Management reporting procedures are adequate.

18. Determine whether computer output is protected from unauthorized access, (i.e,. by placement in locked bins assigned to specific individuals or departments).

EMERGENCY PROCEDURES

19. Review and assess the adequacy of the organization’s emergency procedures.

BACKUP

20. Review procedures for the creation and rotation of backup media (disks or tapes). Coordinate this review with the procedures performed in the Corporate Contingency Planning workprogram in Chapter 10. Determine whether backup procedures provide for the ability to adequately recover:

    a. Operating systems.

    b. Application programs

    c. Master files

    d. Transaction files

    e. System utilities.

    f. Any other programs that are necessary to restore operations at the recovery site.

21. Determine if backup media (disks or tapes) is rotated off-premises in a timely manner.

22. Determine if the off-site storage facility is:

    a. Sufficiently remote from the processing facility.

    b. Adequately controlled for access and environment.

    c. Accessible within a reasonable time frame if backups are needed.

23. Determine whether PC-and LAN-based data and systems backed up as is the mainframe and the backed copies are kept remote from the hardware.

TAPE LIBRARY

24. Determine whether a tape management system is in place.

25. Identify what prevents unauthorized removal, introduction, or substitution of tapes.

26. Identify what prevents the mounting and use of the wrong tape.

27. Identify what prevents the inadvertent use of an active tape as a scratch tape.

28. If a tape management system is in use, verify that only appropriate personnel are able to override its controls, for instance by use of an operating system feature that bypasses processing of the tape's magnetic labels.

ITEM PROCESSING AND DATA ENTRY

29. Determine the adequacy of controls for input and output processing and record retention.

CONCLUSIONS

30. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

31. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

c. Management's proposed actions for correcting deficiencies.

32. Assign rating (see Chapter 5 for additional information).

33. Prepare an index of workpapers for this section of the workprogram.

34. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include, important facts, findings, examiner conclusions, and recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

35. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

___________|________

Reviewer's Initials

Tier II

MANAGEMENT REPORTING AND PLANNING

1. Determine whether performance is reported to management regularly. Obtain a copy of the most recent report(s). They should include:

    a. Response times.

    b. Throughput.

    c. Proportion of downtime.

    d. Frequency and maximum duration of outages.

    e. Proportion, types and causes of job failure.

    f. Computer system peak and average utilization, and trends.

EQUIPMENT MAINTENANCE

2. Review the equipment malfunctions log for patterns of recurring malfunction or repair that have resulted in frequent disruption of operations and/or excessive cost.

3. Review whether management is aware of each problem and has made a decision about whether or how to correct the situation.

OPERATIONAL PROCEDURES

4. Review the operators' duties and determine whether they are prevented from:

    a. Originating entries for processing.

    b. Correcting data exceptions, unposted or rejected items.

    c. Preparing any general ledger and/of subsidiary ledger entries.

    d. Performing any balancing functions (reconcilements) other than run to run control.

    e. Running test programs against live or backup files.

f. Executing programs from the test library during production runs.

g. Controlling report generation and distribution.

5. At entities where one person performs more than one of the above functions, are results checked by an independent person.

6. If operators can override system security are such activities logged and reviewed.

7. Are lengthy and resource-intensive jobs scheduled for execution during non-peak times.

8. Do exceptions to the job schedule require authorization. Are exceptions logged and reviewed.

9. Determine how the source and authorization of production jobs is verified.

10. Are disk packs scanned periodically for obsolete and/or inactive datasets and are those datasets deleted or migrated to tape.

EMERGENCY PROCEDURES

11. Determine if the posted emergency procedures address:

    a. Instructions for shutting off utilities.

    b. Instructions for powering down equipment.

    c. Instructions for activating/deactivating fire suppression equipment.

    d. Personnel evacuation.

    e. Securing valuable assets.

12. Determine if emergency procedures are conspicuously posted throughout the organization.

13. Access whether employees are familiar with their duties and responsibilities in an emergency situation and whether an adequate employee training program been implemented.

14. Determine if the organization periodically conducts drills to test emergency procedures. And access whether drills are monitored to provide feedback on the effectiveness of established emergency procedures and employee training.

TAPE LIBRARY

15. After the expiration date of a tape data set, determine if the data still be read by anyone who knows the identity of the volume.

16. Determine whether:

    a. The tape library is environmentally controlled.

    b. Tapes including backups are tested periodically for defects.

17. Determine if the data center can produce a report showing all tapes on hand and:

    a. How frequently is the inventory updated.

    b. Whether off-site tapes accounted for.

    c. If the inventory includes:

        - Volume name/number.
        - Location.
        - Names of all files on the volume.
        - Creation and expiration dates of the contents.

ITEM PROCESSING AND DATA ENTRY

18. Determine if source document images are recorded for recovery in case the originals are lost in transit.

19. Note whether batch dollar totals are reconciled after processing.

20. Determine if each batch is associated with a responsible individual.

21. Note whether batches are of a reasonable size so that out-of-balance conditions can be reconciled easily.

22. Determine if there is automated checking of data input (e.g. field counts, entry length measurements, reasonable-value tests, etc.).

23. Determine whether reject items are properly segregated from other work.

24. Note whether exception items are adequately controlled and tracked.

25. Assess whether items are allowed to remain in suspense status for extended lengths of time.

26. Proceed to procedure 30, Tier I.

Examiner | Date

____________|_________

Reviewer’s Initials